

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF OREGON**

UNITED STATES OF AMERICA,

Plaintiff,

v.

JOSHAN ROHANI,

Defendant.

Case No. 3:22-cr-00238-IM

**OPINION AND ORDER DENYING
DEFENDANT'S MOTIONS TO
SUPPRESS EVIDENCE AND FOR
FRANKS HEARING**

Natalie K. Wight, United States Attorney, Gary Y. Sussman and Robert S. Trisotto, Assistant United States Attorneys, United States Attorney's Office, 1000 SW Third Avenue, Suite 600, Portland, OR 97204. Attorneys for the Government.

Kevin M. Sali, Kevin Sali LLC, 1500 SW First Ave., Suite 1020, Portland, OR 97201. Attorney for Defendant.

IMMERGUT, District Judge.

Defendant Joshan Rohani is charged with (1) one count of sexual exploitation of children in violation of 18 U.S.C. § 2251(a) and (e); (2) one count of distribution of child pornography in violation of 18 U.S.C. § 2252A(a)(2)(A) and (b)(1); and (3) one count of possession of child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B) and (b)(2). Superseding Indictment,

PAGE 1 – OPINION AND ORDER DENYING DEFENDANT'S MOTIONS TO SUPPRESS EVIDENCE AND FOR *FRANKS* HEARING

ECF 51. On September 7, 2023, Defendant filed his First Motion to Suppress Evidence (“Def.’s First Mot. to Suppress”), ECF 30, and his Motion for *Franks* Hearing (“Def.’s Mot. for *Franks*”), ECF 31. This Court held a status conference on September 12, 2023, setting a briefing schedule for the submitted motions and any further motions to suppress, as well as the dates for oral argument on the motions and for Defendant’s trial. ECF 36. On September 18, 2023, Defendant filed his Second Motion to Suppress Evidence (“Def.’s Second Mot. to Suppress”), ECF 37. On October 20, 2023, this Court heard arguments on Defendant’s motions and denied Defendant’s request for a *Franks* hearing—as explained on the record. ECF 57. At that hearing, this Court conducted a limited evidentiary hearing on Special Agent Clinton Bruce Lindsly’s (“SA Lindsly”) searches of devices seized pursuant to the search warrant. *Id.* This Court addresses Defendant’s Motions to Suppress below.

Defendant moves this Court to suppress all evidence seized pursuant to a search warrant issued on May 23, 2022, and executed the following day. Def.’s First Mot. to Suppress, ECF 30. Defendant argues that the warrant was defective because it failed to establish probable cause and was overbroad. *Id.* Defendant also moves this Court to suppress evidence he claims was seized pursuant to an extension order that lacked legal authority. Def.’s Second Mot. to Suppress, ECF 37. Defendant challenges extension orders in general, arguing that the Fourth Amendment does not permit the extension of a search through a court order. *Id.* at 12–13. He also challenges this extension order in particular, arguing that the Government did not comply with the terms of the search warrant in obtaining the extension order. *Id.* at 8–12, 14–15.

Based on this Court’s review of the pleadings and the arguments of counsel, this Court finds that there was probable cause to support the search of Defendant’s home and person for evidence of possession of child sexual abuse materials, and that the search warrant was not

overbroad. This Court also concludes that, regardless of whether there was probable cause, the federal agents relied on the warrant in good faith. Further, this Court finds that the federal agents relied on the order extending the time to search Defendant's devices in good faith. For the reasons set forth below, this Court DENIES Defendant's First and Second Motions to Suppress.

BACKGROUND¹

A. Homeland Security Investigation in North Carolina

In early November 2021, federal investigators, in conjunction with local law enforcement in North Carolina, executed a state search warrant on an individual suspected of distributing child sexual abuse materials. Application for Warrant, ECF 32-1 at 19–20 ¶¶ 29–31. That individual “admitted to receiving and distributing child pornography.” *Id.* at 20 ¶ 30. Through a note saved on that individual’s cellphone, investigators found a hyperlink for Mega, a file storage and hosting website based in New Zealand. *Id.* at 20 ¶ 31; *id.* at 16 ¶ 22. Mega allows users to upload and share files, as well as create chatrooms in which they can exchange messages and files. *Id.* at 17 ¶¶ 22–23. Content stored on Mega, as well as the chatrooms, are encrypted, meaning they cannot be accessed without a password or a decryption code. *Id.* at 17 ¶¶ 23–24. Due to its end-to-end encryption, Mega “has become a popular cloud-based storage repository and/or location to distribute child pornography.” *Id.* at 18 ¶ 26.

¹ The following facts are taken from Special Agent Rachel Kessler’s affidavit, Application for Warrant, ECF 32-1 at 10–43. To the extent the Government offers new evidence relating to the interpretation of the “hoelaa yooowe” account records, that evidence is beyond the four corners of the affidavit and cannot be considered in determining whether there was probable cause. Facts relating to the warrant extension order are taken from SA Lindsly’s Second Declaration, ECF 42-1, as well as the testimony SA Lindsly gave at the evidentiary hearing, ECF 57.

The Mega hyperlink led investigators to a chatroom named “Trade links.” *Id.* at 20 ¶ 32. Investigators joined the chatroom on November 10, 2021, and for the next two days they observed users discussing and sharing child sexual abuse materials. *Id.* at 20–21 ¶¶ 32–34, 36–39. Sixty-three users were listed on the sidebar of the chatroom as “participants,” including a user with the handle “hoelaa yooowe.” Screenshots of “Trade links” Chatroom, ECF 32-2. When users joined or left the chatroom, a notification appeared in the chat log. Screenshots of “Trade links” Chatroom, ECF 32-2 at 8; Application for Warrant, ECF 32-1 at 21 ¶ 34. As explained above, Mega chatrooms are encrypted, meaning “hoelaa yooowe” could have only joined “Trade links” with a passcode or a link containing the passcode. The investigators did not observe “hoelaa yooowe” chatting or sharing files, but, as stated above, “hoelaa yooowe” was listed as a “participant” on the sidebar of the chatroom. Screenshots of “Trade links” Chatroom, ECF 32-2 at 1–7; *see also* Application for Warrant, ECF 32-1 at 21 ¶ 35. Investigators monitored the “Trade links” chatroom from November 10 to 12, and during that time “almost every video, folder, and/or hyperlink shared by other users contained child pornography.” Application for Warrant, ECF 32-1 at 21 ¶ 34. According to SA Kessler, “[t]here appeared to be no other purpose for this chatroom other than distributing child pornography.” *Id.* Law enforcement requested that Mega decommission the chatroom and files shared in it. Application for Warrant, ECF 32-1 at 24 ¶ 40.

B. Homeland Security Investigation in Oregon

The “hoelaa yooowe” user was paying Mega for increased online storage capacity, which allowed investigators to link the account to Defendant. *Id.* at 24–25 ¶ 41. Mega “does not respond to legal process from the United States but provides basic subscriber records to law enforcement.” *Id.* at 17 ¶ 24. According to the account records, Defendant created the “hoelaa

yooowe” account in July 2021. *Id.* at 27 ¶ 47. “Hoelaa yooowe” was a participant in thirty-four other chatrooms and had “approximately 2,070 GB of stored data, 367,398 files (i.e. photographs and/or videos), and 6,714 folders.” *Id.* at 24–25 ¶ 41. As affiant Special Agent Rachel Kessler (“SA Kessler”) explained, this amount of data is “consistent with massive downloading of photographs and/or video files.” *Id.*

Investigators also reviewed access logs for “hoelaa yooowe” provided by Mega. *Id.* at 25 ¶¶ 41–42. Based on the information SA Kessler had available to her when she was completing the warrant affidavit, she concluded that Defendant accessed his Mega account (but not necessarily the “Trade links” chatroom) at least 40 times between the creation of the account in July 2021, and the closing of the account by Mega on November 18, 2021. *Id.* at 25–27 ¶ 42, 44, 47. SA Kessler also included that the “hoelaa yooowe” account had been accessed by a particular IP address on August 15, September 10, October 16, and November 16, 2021. *Id.* at 28 ¶ 47. Subscriber records linked that IP address to Defendant’s residence. *Id.* at 28 ¶ 48.

Investigators also identified another Mega account associated with Defendant. That account had been created in January 2019 and was suspended in August 2019 “due to ‘moderator status of emergencytd chat link 77hjxC4t,’” which SA Kessler “believe[d] to have contained child pornography.” *Id.* at 28–29 ¶ 49. She based this belief on her “review of dozens of other M[ega] account subscriber records, conversations with M[ega] staff, and conversations with other law enforcement officers.” *Id.* Elsewhere in the affidavit, SA Kessler explained that “persons involved in the receipt, collection, and distribution of child pornography often have multiple M[ega] accounts,” *id.* at 18 ¶ 26, and that Mega will “suspend [an] account” if it “determines that [a reported] link contains child pornography or violates [its] terms of service,” *id.* at 17 ¶ 24.

Based on this information, SA Kessler concluded that she had probable cause to believe Defendant had possession of, or accessed with intent to view, child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B), and that evidence of this violation would be located on devices kept at Defendant's residence and on his person. *Id.* at 42 ¶ 73. Magistrate Judge Jolie Russo issued the warrant on May 23, 2022. Warrant, ECF 32-4. The following day, federal agents searched Defendant's residence and person and seized around 52 digital devices. First Declaration of Clinton Bruce Lindsly ("First Lindsly Decl."), ECF 43-2 at 6 ¶ 17. Agents found child sexual abuse materials on some of those devices. *Id.* Defendant was originally indicted on July 13, 2022. Indictment, ECF 2. The Government filed a superseding indictment on October 17, 2023. Superseding Indictment, ECF 51.

C. Completion of Search Through Extension Order

By its terms, the warrant required law enforcement personnel to "perform an initial search of the original digital device or image within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant." Warrant, ECF 32-4 at 9 ¶ 22(f). That 120-day period would have ended on September 21, 2022. If that initial search indicated that the digital device contained data "falling within the list of items to be seized pursuant to this warrant," the device was to be retained by the Government. *Id.* at 9–10 ¶ 22(f). The Government could "seek an extension of the time period from the Court within the original 120-day period from the date of the execution of the warrant" if it needed additional time to perform an initial search of a device or devices. *Id.* at 10 ¶ 22(f). The warrant required law enforcement to "complete the search of the digital device or image within 180 days of the date of execution of the warrant." *Id.* That 180-day period would have ended on November 20, 2022. The

Government could “seek an extension of the time period from the Court” if it needed additional time to complete the search of a digital device or devices. *Id.*

Several days prior to the expiration of the 180-day period, in November 2022, SA Lindsly contacted the United States Attorney’s Office “to request an extension of time to finish [his] review.” Second Declaration of Clinton Bruce Lindsly (“Second Lindsly Decl.”), ECF 42-1 at 4 ¶ 9. SA Lindsly noted that he was not requesting additional time to review two devices that were not initially searched within the 120-day period for initial searches. *Id.* During the limited evidentiary hearing conducted on Defendant’s Second Motion to Suppress, SA Lindsly testified to the same. ECF 57. On January 12, 2023, about eight weeks after the expiration of the 180-day period, the Government moved for an extension of time to complete its search of the seized digital devices. Motion for Extension of Time to Complete Search and Forensic Analysis of Digital Devices (“Gov.’s Mot. for Extension of Time”), ECF 38-2. Magistrate Judge Jeffrey Armistead granted the Government’s motion, ordering that the Government “shall have 180 days from the date of this Order to complete the searches and forensic analyses of the digital devices seized pursuant to the search warrant.” Order, ECF 38-6. Law enforcement “did not continue reviewing any digital devices seized under the warrant after the 180-day period lapsed until [the] extension was granted.” Second Lindsly Decl., ECF 42-1 at 4 ¶ 10. That 180-day period would have ended on July 12, 2023. Federal agents fully completed the search on May 3, 2023. *Id.* at 4 ¶ 11.

LEGAL STANDARDS

The Fourth Amendment provides that “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.” *United States v. Jones*, 565 U.S. 400, 404 (2012). To support the issuance of a search

warrant, an affiant must present evidence that gives the judge a ““substantial basis for concluding’ probable cause existed” based on the totality of the circumstances. *United States v. Underwood*, 725 F.3d 1076, 1081 (9th Cir. 2013) (alterations omitted) (quoting *Illinois v. Gates*, 462 U.S. 213, 238–39 (1983)).

This test requires a “common sense determination that ‘there is a fair probability that contraband or evidence of a crime will be found in a particular place.’” *United States v. Mendonsa*, 989 F.2d 366, 368 (9th Cir. 1993) (quoting *Gates*, 462 U.S. at 238); *see also United States v. Norris*, 942 F.3d 902, 910 (9th Cir. 2019) (“Probable cause to search a location exists if, based on the totality of the circumstances,’ a ‘fair probability’ exists that the police will find evidence of a crime.” (quoting *United States v. Perkins*, 850 F.3d 1109, 1119 (9th Cir. 2017))); *United States v. Seybold*, 726 F.2d 502, 503 (9th Cir. 1984) (explaining that the totality of the circumstances test requires a reviewing court to “make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place” (alteration in original) (citing *Gates*, 462 U.S. at 238)).

While a court is free to draw “reasonable inferences” from the materials supplied to it, *see Gates*, 462 U.S. at 240, “all data necessary to show probable cause . . . must be contained within the four corners of a written affidavit given under oath.” *United States v. Anderson*, 453 F.2d 174, 175 (9th Cir. 1971); *see also United States v. Gourde*, 440 F.3d 1065, 1067 (9th Cir. 2006) (en banc). “[T]he task of a reviewing court is not to conduct a de novo determination of probable cause, but only to determine whether there is substantial evidence in the record supporting the magistrate’s decision to issue the warrant.” *Massachusetts v. Upton*, 466 U.S. 727, 728 (1984) (per curiam); *see also Gourde*, 440 F.3d at 1069 (noting that reviewing courts

“are not in a position to flyspeck the affidavit through de novo review” and that “the magistrate judge’s determination ‘should be paid great deference’” (quoting *Gates*, 462 U.S. at 236)).

Nevertheless, conclusory statements regarding the affiant’s beliefs are no substitute for facts the court can meaningfully evaluate. *Underwood*, 725 F.3d at 1082–83 (collecting cases).

DISCUSSION

A. First Motion to Suppress

Defendant challenges the lawfulness of the warrant on two grounds. First, he argues that SA Kessler’s affidavit was insufficient to establish anything more than his “mere propinquity” to illegal activity, much less probable cause. Def.’s First Mot. to Suppress, ECF 30 at 14–20. Second, he argues that the warrant was an invalid general warrant. *Id.* at 27–30. As explained below, neither of these arguments is availing.

1. The Warrant Provided Sufficient Information for an Individualized Probable Cause Determination

Defendant likens the circumstances here to cases in which courts found probable cause lacking because an affidavit established nothing more than “mere propinquity” to illegal activity. *See* Def.’s First Mot. to Suppress, ECF 30 at 15–20 (first discussing *Ybarra v. Illinois*, 444 U.S. 85 (1979); and then discussing *United States v. Collins*, 427 F.3d 688 (9th Cir. 2005)). And Defendant distinguishes the circumstances here from a case in which the Ninth Circuit found probable cause for a search involving child sexual abuse materials. *See* Def.’s First Mot. to Suppress, ECF 30 at 14–15 (discussing *Gourde*, 440 F.3d 1065).

In drawing these comparisons, Defendant omits pertinent information from SA Kessler’s affidavit. For instance, while the “Trade links” chatroom may have had an “entirely generic name” and “was available through lawfully and commonly available applications and services,” *see* Def.’s First Mot. to Suppress, ECF 30 at 15, it was also encrypted. Defendant could not have

stumbled upon it, but rather would have needed the passcode or hyperlink containing the passcode to access it. *See Application for Warrant*, ECF 32-1 at 17 ¶ 23. Investigators likewise did not stumble upon it—they gained access to the “Trade links” chatroom because the encrypted hyperlink was saved on the phone of someone who admitted to possessing and distributing child sexual abuse materials. Once in the chatroom, investigators observed the users trading and discussing such materials, and based on those messages, files, and links shared in the “Trade links” chatroom, SA Kessler concluded that “[t]here appeared to be no other purpose for this chatroom other than distributing child pornography.” *Id.* at 21 ¶ 34. One could reasonably expect than anyone who innocently “stumbled upon” a chatroom in which images of child sexual abuse was shared would immediately leave the chatroom, not remain as a “participant.”

Further, Defendant does not mention that the affidavit included information about another Mega account registered to Defendant.² *See id.* at 28–29 ¶ 49. That account “had been suspended” just two years earlier “due to ‘moderator status of emergencytd chat link 77hjxC4t,’” which SA Kessler “believe[d] to have contained child pornography.” *Id.* She based this belief on her “review of dozens of other M[ega] account subscriber records, conversations with M[ega] staff, and conversations with other law enforcement officers.” *Id.* Elsewhere in the affidavit, SA Kessler explained that Mega will “suspend [an] account” if it “determines that [a reported] link contains child pornography or violates [its] terms of service.” *Id.* at 17 ¶ 24. This was

² On reply, Defendant claims for the first time that SA Kessler’s conclusion about the suspended account is unaccompanied by underlying facts and thus cannot be relied upon for the probable cause determination. Claims raised on reply are waived. *See United States v. Romm*, 455 F.3d 990, 997 (9th Cir. 2006) (declining to consider an issue “because ‘arguments not raised by a party in its opening brief are deemed waived’” (quoting *Smith v. Marsh*, 194 F.3d 1045, 1052 (9th Cir. 1999))). Regardless, this Court finds that the information provided by SA Kessler was sufficient to allow the Magistrate Judge to assess SA Kessler’s conclusion.

information, individualized to Defendant, which the Magistrate Judge could consider when deciding whether the affidavit established probable cause.

Moreover, while Defendant casts his having a Mega account as indicative of nothing more than use of a lawful online service, such innocent activity, though not conclusive of probable cause, may “provide the basis for a showing of probable cause” when considered in the context of all the surrounding circumstances. *See Gates*, 462 U.S. at 245 n.13. The Magistrate Judge was entitled to rely on SA Kessler’s training and experience when interpreting seemingly innocent conduct. *See United States v. Hay*, 231 F.3d 630, 636 (9th Cir. 2000) (citing *United States v. Gil*, 58 F.3d 1414, 1418 (9th Cir. 1995)). As SA Kessler explained in the search warrant affidavit, her training and experience taught her that Mega is a popular site for storing and sharing child sexual abuse materials, that collectors of child sexual abuse materials often maintain their collections through cloud-based file storing services like Mega, and that the “hoelaa yooowe” account had an amount of stored data consistent with massive downloading of photographs and/or video files. The Magistrate Judge was entitled to consider all of this information in determining whether Defendant’s conduct was merely innocent or provided a basis for finding probable cause.

Based on the affidavit as a whole, this Court finds it was reasonable to infer that Defendant used Mega to possess and/or access child sexual abuse materials with the intent to view them, and that there was a fair probability that evidence of that offense would be found on the digital devices he kept on his person and in his home. *See United States v. Martin*, 327 F. App’x 740, 742 (9th Cir. 2009) (“[I]t was reasonable to infer that Martin was the individual who visited several different internet relay chat . . . channels within a short time period that were all known to Customs Service agents to be used for exchanging child pornography, and there was a

‘fair probability’ that such an individual would possess child pornography on his home computer.”). As the Ninth Circuit has explained, the “resolution of doubtful or marginal cases in this area should ‘largely be determined by the preference to be accorded to warrants.’” *United States v. Kelley*, 482 F.3d 1047, 1050–51 (9th Cir. 2007) (quoting *Gates*, 462 U.S. at 237 n.10). This Court resolves this case accordingly, giving substantial deference to the Magistrate Judge’s probable cause determination.

2. The Good-Faith Exception Applies

Even if this Court found that the search warrant lacked probable cause, the good-faith exception to the exclusionary rule applies. In *United States v. Leon*, the Supreme Court set out an exception to the exclusionary rule for a search conducted in good faith reliance upon an objectively reasonable search warrant. 468 U.S. 897 (1984). The Government bears the burden of proving that officers relied on the search warrant “in an objectively reasonable manner.” *United States v. Crews*, 502 F.3d 1130, 1136 (9th Cir. 2007) (citing *United States v. Clark*, 31 F.3d 831, 835 (9th Cir. 1994)); *see also United States v. Huggins*, 299 F.3d 1039, 1047 (9th Cir. 2002) (“Application of the good faith exception is particularly appropriate in the instant case because the legal question of whether probable cause existed is a close one,’ while the objective reasonableness of the officers’ reliance on the warrant is more straightforward.” (citation omitted)).

In four circumstances, the good-faith exception will not apply because reliance is per se unreasonable:

- (i) where an affiant misleads the issuing magistrate or judge by making a false statement or recklessly disregarding the truth in making a statement; (ii) where the magistrate or judge wholly abandons her judicial role in approving the warrant, acting only as a “rubber stamp” to the warrant application rather than as a neutral and detached official; (iii) where the warrant is facially deficient in

detail as to the place to be searched or the things to be found that the officers could not reasonably presume it to be valid; or (iv) where the affidavit upon which the warrant is based is so lacking in indicia of probable cause that no reasonable officer could rely upon it in good faith.

Id. (citing *Leon*, 468 U.S. at 923–26). Defendant identifies two of these circumstances which he claims render the good-faith exception inapplicable.

First, he argues that the exception “does not apply because the deficiencies in the application were sufficiently plain to make officers’ reliance on the warrant unreasonable.” Def.’s First Mot. to Suppress, ECF 30 at 22 (citing *United States v. McGrew*, 122 F.3d 847, 850 (9th Cir. 1997)). Showing that a warrant is so lacking in indicia of probable cause that no reasonable officer would rely on it is a heavy burden because, “[i]n the ordinary case, an officer cannot be expected to question the magistrate’s probable-cause determination or his judgment that the form of the warrant is technically sufficient.” *Leon*, 468 U.S. at 921. As this Court has already explained, the affidavit contained sufficient information to “establish at least a colorable argument for probable cause.” *United States v. Grant*, 682 F.3d 827, 836 (9th Cir. 2012) (quoting *United States v. Luong*, 470 F.3d 898, 903 (9th Cir. 2006)). Considering that information, a reasonable officer could rely on the warrant in good faith.

Second, Defendant claims that the good-faith exception does not apply because the Magistrate Judge “was misled by information that SA Kessler ‘knew was false or would have known was false except for h[er] reckless disregard for the truth.’” Def.’s First Mot. to Suppress, ECF 30 at 22 (alteration in original) (quoting *Leon*, 468 U.S. at 923). While Defendant may quibble with aspects of the affidavit like the phrasing of the appearance of “hoelaa yooowe” in the “Trade links” chatroom or the account activity logged in Mega’s records, this does not mean that SA Kessler knowingly or recklessly presented false information. As this Court explained at

the October 20, 2023 hearing, Defendant has not shown that SA Kessler intentionally misled the Magistrate Judge or exhibited a reckless disregard for the truth.

Further, this Court notes that the United States Attorney's Office approved the warrant prior to it being signed by the Magistrate Judge. *See* SA Kessler Declaration, ECF 43-1 at 5 ¶ 16; First Lindsly Decl., ECF 43-2 at 6 ¶ 16. The Ninth Circuit has explained that law enforcement's reliance on counsel can be "critical" to finding good faith. *United States v. Winsor*, 549 F. App'x 630, 632 (9th Cir. 2013) (citing *United States v. Brown*, 951 F.2d 999, 1005 (9th Cir. 1992)). Ultimately, even if the warrant lacked probable cause, the good-faith exception to the exclusionary rule applies.

3. The Warrant Was Not an Invalid General Warrant

Defendant also argues that the warrant was impermissibly broad, amounting to an invalid general warrant and requiring suppression of all evidence seized pursuant to it. *See* Def.'s First Mot. to Suppress, ECF 30 at 27–30.

"The Fourth Amendment requires that a warrant particularly describe both the place to be searched and the person or things to be seized." *United States v. Smith*, 424 F.3d 992, 1004 (9th Cir. 2005) (citation omitted). "The purpose of the breadth requirement is to limit the scope of the warrant by the probable cause on which the warrant is based." *Id.* (citation and internal quotation marks omitted). In applying the breadth requirement, the Ninth Circuit has repeatedly held that warrants similar to the one at issue here were not overbroad. *See United States v. Schesso*, 730 F.3d 1040, 1046 (9th Cir. 2013) (holding that the seizure and subsequent off-premises search of an entire computer system and associated digital storage devices was justified because "[t]he government was faced with the challenge of searching for digital data that was not limited to a specific, known file or set of files" and "[t]he government had no way of knowing which or how

many illicit files there might be or where they might be stored, or of describing the items to be seized in a more precise manner” (citation omitted)); *Hay*, 231 F.3d at 637–38 (rejecting an overbreadth challenge to a “wholesale search and seizure of [the defendant’s] apartment and computer system” and reasoning that the “application did not ask for, and the warrant did not authorize, seizure of every document, but of child pornography which is a sufficiently specific definition to focus the search”); *United States v. Lacy*, 119 F.3d 742, 746–47 (9th Cir. 1997) (holding that a warrant “authoriz[ing] the seizure of [an] entire computer system” was not overbroad because the affidavit “established probable cause to believe [the] entire computer system was likely to evidence criminal activity,” the warrant “contained objective limits to help officers determine which items they could seize,” and no more precise description of the computer equipment sought was possible).

The warrant here was not unconstitutionally overbroad. The search and seizure were sufficiently focused by the objective limits of the target offense, and the Government could not have provided greater specificity because it did not know how many illicit files there might be or where those files might be stored.

B. Motion for *Franks* Hearing

Defendant urges this Court to grant a *Franks* hearing because, according to him, SA Kessler’s affidavit intentionally or recklessly contained false statements and misleading omissions that were crucial to the Magistrate Judge’s determination of probable cause. Def.’s Mot. for *Franks*, ECF 31 at 2–11 (citing *Franks v. Delaware*, 438 U.S. 154, 155–56 (1978)). In *Franks v. Delaware*, the Supreme Court established the principle that a defendant is entitled to a *Franks* hearing only if he makes a twofold showing. 438 U.S. at 155–56. First, he must make a “substantial preliminary showing that a false statement knowingly and intentionally, or with

reckless disregard for the truth, was included by the affiant in the warrant affidavit.” *Id.*; *see also United States v. Saterstad*, 852 F. App’x 250, 251 (9th Cir. 2021). Second, the defendant must demonstrate that “the false or misleading statement or omission was material, *i.e.*, ‘necessary to finding probable cause.’” *Perkins*, 850 F.3d at 1116 (quoting *United States v. Martinez-Garcia*, 397 F.3d 1205, 1214–15 (9th Cir. 2005)). If the defendant meets his burden by making these two showings, then he is entitled to a *Franks* hearing. Then, if the defendant makes those two showings by a preponderance of the evidence, the affidavit’s false material will be set aside, and the remaining content will be judged to see if it is insufficient to establish probable cause. *Id.*; *see also United States v. Chesher*, 678 F.2d 1353, 1362 (9th Cir. 1982).

As this Court already explained on the record at the October 20, 2023, hearing held on the instant motion, Defendant is not entitled to a hearing under *Franks*. Defendant has not substantially shown that SA Kessler intentionally or recklessly made any false statements or misleading omissions, nor that those allegedly false statements and misleading omissions were material to the probable cause determination.

C. Second Motion to Suppress

Defendant seeks the suppression of all evidence seized pursuant to an extension order allowing law enforcement additional time to complete the search of his devices. He makes a general argument and a specific argument. In general, he argues that there exists no legal authority for such extension orders, and, even if there were legal authority, the extension order here “could not pass constitutional scrutiny.” Def.’s Second Mot. to Suppress, ECF 37 at 12–15. Specifically, he argues that for several devices the initial search was not completed within the appropriate timeframe and so “the Government’s authority to search th[ose] items . . . had expired and could not be revived consistent with the Warrant’s terms.” Def.’s Second Mot. to

Suppress, ECF 37 at 8–11 (discussing items listed in Lines 5, 6, and 11 of a Homeland Security Investigations Report of Investigation); *see also* ECF 57 (introducing during evidentiary hearing Defendant’s Exhibit 104, a Homeland Security Report of Investigation from May 2022, and identifying disputed devices).

By its terms, the warrant required law enforcement personnel to “perform an initial search of the original digital device or image within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant.” Warrant, ECF 32-4 at 9 ¶ 22(f). If that initial search indicated that the digital device contained data “falling within the list of items to be seized pursuant to this warrant,” the device was to be retained by the Government. *Id.* at 10 ¶ 22(f). The Government could “seek an extension of the time period from the Court within the original 120-day period from the date of the execution of the warrant” if it needed additional time to perform an initial search of a device. *Id.* The warrant required the law enforcement personnel to “complete the search of the digital device or image within 180 days of the date of execution of the warrant.” *Id.* The Government could “seek an extension of the time period from the Court” if it needed additional time to complete the search of a digital device. *Id.* While the warrant set a deadline for seeking additional time to perform the initial search, “within the original 120-day period from the date of the execution of the warrant,” it did not set a deadline for seeking additional time to complete the search. The Government moved for an extension of time to complete the search on January 12, 2023. Gov.’s Mot. for Extension of Time, ECF 38-2, and Magistrate Judge Jeffrey Armistead granted it, Order, ECF 38-6. The Government completed the search within that timeframe.

1. This Court Declines to Decide Whether the Extension Order Was Legally Authorized

Defendant argues that “there does not appear to be any authority suggesting that” extension orders are “constitutionally cognizable.” Def.’s Second Mot. to Suppress, ECF 37 at 13. He points out that the Fourth Amendment, the case law interpreting that amendment, and Federal Rule of Criminal Procedure 41 all “refer specifically to warrants, not orders.” *Id.* Defendant suggests that “the only legally valid way to extend the searching or seizing authority from an initial warrant is to secure a follow-up warrant.” *Id.*

In response, the Government gestures to analogous situations and cases, but it does not provide a source of legal authority for the extension order. It describes the filing of a motion requesting additional time to complete a search as “standard practice in this district when seeking extensions of time to search digital devices,” but it provides no support for this claim. *See* Government’s Response to Defendant’s Second Motion to Suppress (“Gov.’s Resp. to Def.’s Second Mot. to Suppress”), ECF 42 at 5. It notes that “courts extend the time during which the United States is authorized to intercept wiretap communications by court order,” but, as the Government’s citation indicates, that practice is based on a statute—legal authority for that practice. *Id.* at 15 (citing 18 U.S.C. § 2518(1), (5)). The Government also points this Court to *United States v. Syphers*, 426 F.3d 461 (1st Cir. 2005), a First Circuit case dealing with a one-year extension order issued by a state court to allow for the search of a seized computer. *Id.* at 469. *Syphers* is not binding on this Court, nor does it appear to discuss the question of legal authority underlying extension orders.

Because this Court concludes that the good-faith exception applies, explained below, it declines to decide whether the extension order obtained here was a valid method for seeking additional time from the court to complete the search. However, this Court notes that, aside from PAGE 18 – OPINION AND ORDER DENYING DEFENDANT’S MOTIONS TO SUPPRESS EVIDENCE AND FOR FRANKS HEARING

the question of the legality of extension orders, the total duration of this search was reasonable under the Fourth Amendment. The probable cause that justified the initial seizure of the devices continued to justify the later search after the 180-day period elapsed. *See United States v. Nepstead*, 424 F.2d 269, 271 (9th Cir. 1970); *United States v. Jennen*, 596 F.3d 594, 600 (9th Cir. 2010) (“Because there was no unreasonable delay in executing the warrant and the facts underlying the magistrate’s determination of probable cause did not materially change, there was no need . . . for [law enforcement] to confer with a judicial officer to see if probable cause still existed.” (alterations, quotation marks, and citation omitted)), *abrogated on other grounds by Descamps v. United States*, 570 U.S. 254 (2013), and *Mathis v. United States*, 579 U.S. 500 (2016). The circumstances providing probable cause to seize the devices and search for electronically stored data did not dissipate or go stale in the time it took law enforcement to complete the search. Further, the reason for the delayed search was unrelated to probable cause—as SA Lindsly testified, investigators had hundreds of thousands of files to review and the delay was due to the time-intensive nature of the search. *See* Second Lindsly Decl., Ex. 6, 42-1 at 4 ¶¶ 4–5.

2. The Good-Faith Exception Applies

Even if no legal authority existed allowing for the extension order here, the federal agents nonetheless relied on it in good faith. Contrary to Defendant’s assertion that federal agents were acting outside the warrant’s scope, and so the good-faith exception does not apply, Def.’s Second Mot. to Suppress, ECF 37 at 15–16, by its own terms the warrant allowed for extensions of time to be sought. The federal agents complied with the warrant’s temporal scope—they performed initial searches within 120 days of the execution of the warrant—and, as the warrant provided, they sought additional time to complete the search of those devices. For the devices they did not

initially search within the 120-day window, they ceased reviewing those devices after that window expired and never resumed their review. Only after being granted the extension did the agents resume their search of the permitted devices, and they completed that search within the temporal scope established by the extension order.

This is true even for the items Defendant claims were improperly searched pursuant to the extension order. *See* Def.’s Second Mot. to Suppress, ECF 37 at 5 (arguing that “the search prescribed in paragraph 22(f) of the Warrant does not appear to have been conducted as to the items identified in Lines 5, 6, and 11” within the appropriate timeframe); ECF 57 (introducing at evidentiary hearing Defendant’s Exhibit 104 and identifying disputed devices). The Government counters that initial searches of those devices occurred before the 120-day window expired, and that those initial searches revealed that each device contained items to be seized pursuant to the warrant. Gov.’s Resp. to Def.’s Second Mot. to Suppress, ECF 42 at 4; Second Lindsly Decl., ECF 42-1 at 2–3 ¶ 7. The Government suggests that Defendant misreads the investigation reports. Gov.’s Resp. to Def.’s Second Mot. to Suppress, ECF 42 at 8 n.3. This Court agrees with the Government’s reading of the record. Based on SA Lindsly’s testimony and the investigation reports, law enforcement personnel initially searched the contested items and located responsive materials before the initial 120-day period elapsed. Federal agents then sought additional time to complete the search. Thus, under the terms of the warrant, the extension order was properly sought, and the items were searched within the timeframe provided by that extension order. All of this indicates that the agents were conforming their conduct based on their good-faith belief in the legitimacy of a search warrant and extension order issued by a detached and neutral magistrate judge.

Further, while law enforcement officials must have a reasonable knowledge of what the law prohibits, *see* Def.’s Second Mot. to Suppress at 16–17, it is not clear that the law prohibits this warrant extension practice. As SA Lindsly explained, he was in contact with the United States Attorney’s Office regarding the motion for extension of time before the expiration of 180-day period provided for in the warrant, and the United States Attorney’s Office filed the motion seeking the extension of time. Second Lindsly Decl., ECF 42-1 at 4 ¶ 9; Gov.’s Mot. for Extension of Time, ECF 38-2. It was reasonable for law enforcement officials to rely on the judgment of attorneys and a magistrate judge in concluding that an extension order was a proper method for complying with the warrant’s provisions.

At bottom, the exclusionary rule is triggered when law enforcement conduct is “sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system.” *Herring v. United States*, 555 U.S. 135, 144 (2009). The error alleged here does not rise to that level; the agents’ conduct was not so objectively culpable as to require exclusion.

CONCLUSION

For the foregoing reasons, this Court DENIES Defendant’s First Motion to Suppress, ECF 30, Motion for *Franks* Hearing, ECF 31, and Second Motion to Suppress, ECF 37.

IT IS SO ORDERED.

DATED this 2nd day of November, 2023.

/s/ Karin J. Immergut
Karin J. Immergut
United States District Judge